

Audio Steganography for Secure Data Transmission

Kundu N.^{1*} and Kaur A.²

^{1*}Dept. CST, Central University of Punjab, Bathinda, Punjab, India

²Dept. CST, Central University of Punjab, Bathinda, Punjab, India

*Corresponding Author: nisha.kundu26@gmail.com

Available online at: www.ijcseonline.org

Received: 02/Jan/2017

Revised: 05/Feb/2017

Accepted: 21/Feb/2017

Published: 28/Feb/2017

Abstract—As the internet growing day by day secure transmission of information is crucial. Steganography and cryptography both techniques provide data confidentiality, integrity and help us to protect data from day by day attacks. Internet communication has become an essential part of infrastructure now a days and also lots of applications are internet based. So the communication made must be secret to avoid attacks. Steganography is a process of hiding the information of secret messages or one can say that it is an art of sending the hidden data or message over a public network. In the proposed approach message is first encrypted through using The Vigenere Square Encryption Algorithm. After those characters of information or data is embedded into deeper layers through modified LSB method. After that further audio transposition encryption technique is used for audio and accuracy for transposition method is measured in terms of MSE.

Keywords— Audio Steganography, Encryption, Audio Encryption, Modified LSB, Vigenere Square Encryption Algorithm, LSB Coding , PSNR-Peak signal to noise ratio, MSE-mean square error

I. INTRODUCTION

Internet communication is important part of communication now a day. So Data needs to be protected and secure when it is transmitted over the public network. By using security technique data integrity , confidentiality is to be maintained [1] and steganography is proposed to provide more security to the data .Audio steganography is a technique in which the secret data is embedded into the cover audio by using various techniques like LSB, with the secret message hidden from the unauthorized party and to protect against the attacks. The main requirements for any steganographic system are - transparency, hiding capacity and robustness [2].At the receiver's side the hidden data can be extracted from the stego signal using the reverse algorithm as that of used for embedding. Encryption is done for more security of data and information travelled through a public network. Encryption is a part of cryptography .Cryptography provides data confidentiality, data integrity and in the proposed approach combination of encryption and steganography is used [4-5]. The proposed method works on modified vigenere cipher technique. The Vigenere square cipher encrypts its inputs by using the key and the plaintext as indices into a fixed lookup table: the Vigenere square [3]. After that the message characters are converted to ASCII values and then embedding is done into the deeper layers using modified LSB method. For more security further audio encryption is done by using transposition method [6] [7]. Finally MSE and PSNR are calculated so that we can compare the results with other methods. After embedding of message is done, the stego audio is obtained by use of various steganographic methods [8][9].

II. RELATED WORK

Authors in [10] told about LSB basic method that how embedding is done using basic method and also the Capacity of LSB-Based Audio Steganography .To extract a secret message from an LSB encoded sound file, the receiver needs to use same approach as used in the embedding process. Normally, the length of the secret message to be encoded is smaller than the total number of samples in a sound file. One must decide then on how to choose the subset of samples that will contain the secret message.

Authors in 2010 presented a scheme that uses an image file as the secret data to be hidden inside the audio file i.e. called cover object. Image is chosen because the size of the image is generally quite small as compared to audio [11] in which it must be hidden. The proposed method is based on the basic technique for hiding secret data in audio i.e. LSB. According to the proposed method, least significant bits up to three LSB positions are used as a stego-key to encode the image bits in stego-object. Thus, the image data can be embedded according to the embedding algorithm taking various MSB positions and same process is used for receiver end.

Authors in 2011 purposed Discrete Wavelet Transform (DWT) Audio steganography method so that data is embedded with signal in the LSBs of the wavelet coefficients of audio signal [12]. To improve the inaudibility of embedded data employed a hearing threshold when hiding data in the integer wavelet coefficients, while avoided data hiding in the silent parts of audio signal. In this method robustness is achieved and here due the presence of hearing

threshold the inaudibility is also improved, so it is better than that of HAS and that of above one in term of security too.

Authors in, 2011 purposed an algorithm in which the secret data is first encrypted using AES algorithm [13]. This encrypted data is then embedded into an audio file using basic LSB technique. The authors then encrypt the audio file using Spread Spectrum technique before transmitting it over the network. So this will help in enhancement of the security of secret message so that we can protect the message against stego based attacks.

In [14], authors have suggested an algorithm in which the data is first subjected to encryption using Data Encryption Standard (DES). The encrypted message is then passed to embedding phase. In embedding phase the encrypted message will be embedded into the cover medium which is either image or audio or video resulting in a stego medium. The embedded stego medium contains the encrypted text message which is extracted at the receiver side. The extracted text is decrypted using decryption module.

Authors in 2012 proposed a three layered model for audio steganography based on least significant bit replacement [15]. In this purposed research the secret message to be transmitted is passed through two layers before it is embedded within the cover message in the third layer. The stego(secret message after applying the steganography) message is transmitted over the network to the receiver side. The objective of the paper is to make sure the confidentiality of the secret message. As we know confidentiality is equivalent to privacy. Measures are used to ensure confidentiality to prevent sensitive information from reaching to the wrong people. Access must be restricted to the authorized people and take care of capacity, transparency and robustness.

Authors in 2012 proposed method that adapts the Frequency Masking concept using an efficient sorting of the wavelet coefficients of the secret messages and use an indirect LSB substitution for hiding speech signals into speech signals [16]. The proposed method contains four steps: decomposition and pre-scaling by transforming the decimal coefficients of the signals to a binary representation by the Discrete Wavelet Transform (DWT), then using an efficient sorting of the wavelet coefficients of the secret messages, then using an indirect LSB substitution for hiding speech signals into speech signals, and finally reconstruct the signals and post-scaling it by applying the inverse wavelet transform.

Authors in 2012 presented a novel approach of submission technique of audio Steganography [17]. Using genetic algorithm, message bits are embedded into multiple and

higher LSB layer values based on algorithm that embed data into deeper LSB bits which is resulting in increased robustness. By using this purposed method the robustness would be increased against those intentional attacks which try to reveal the hidden message and also some unintentional attacks like noise addition as well. So overall the integrity and security and robustness are maintained by using this approach because the hidden message is not under the insecurity of attacks to change it.

Authors in [18] proposed technique, the sound is divided into samples where each sample is of 24bit, 8 bits are to be hidden in each sample by distributing the bit pattern [18] that corresponds to the secret gray scale image across the LSBs of the pre-processed sound samples (i.e. the pre-processed sound waves take the shape of a RGB colored image). So the embedding capacity is 8 bits per audio sample which results in large embedding capacity. Additionally, hiding the secret bit pattern by distributing it in the layers of the colored image, add more secrecy to the hidden data.

Authors in [19] proposed a method in which consecutive LSB's in each sample of cover audio is replaced with secret message bit. LSB method is very easy to implement but have low robustness. The paper also compares the spectra of original audio signal before embedding and audio signal after embedding and compares the results by using various audio specifications.

Authors in [20] discussed a method of hiding text or secret in audio using multiple LSB steganography and provide security using cryptography techniques. The research has proposed two approaches of substitution technique of audio steganography that improves the capacity of cover audio for embedding data. Here message bits are embedded into multiple and variable LSBs. From the results these methods improve the capacity of data hiding of cover audio.

Authors [21] studied a detailed look of audio steganography techniques using LSB and genetic algorithm approach. This research has study of various techniques of audio steganography using different algorithms like genetic algorithm approach and LSB approach. It has tried some approaches that help in audio steganography. It has the art and science of writing hidden messages in such a way that only the sender and intended recipient suspects the existence of the message.

Authors in [22] proposed, dual layer randomization approach. First layer of randomization is achieved by randomly selecting the byte number or samples from all. An additional layer of security is provided by randomly selecting the bit position at which embedding is done in the selected samples. Using this proposed algorithm the transparency and robustness of the steganographic technique is increased. Due

to less robustness and more vulnerability to be attacked LSB method is not preferred much. Instead two bits (2nd and 3rd LSB's) are used for hiding message. This method is good in terms of integrity and robustness also. A filter is designed to minimize the changes occurred in stego file using a unique key. By this unique key the security of data hiding is increased. The key will derive to extract the correct message at receiver's end. So this method provides more security than that of the LSB method used earlier [23][24].

Authors in [25] proposed a new approach that overcomes the problems of substitution techniques in audio steganography one problem is that they are less robust against intentional attacks that try to reveal hidden message and second problem is having low robustness against unintentional attacks. The algorithm will hide the message as per the proposed solution (in deeper layers of audio sample and will modify other bits to minimize the error). The method currently uses 2 bits per byte of audio sample. This will progress towards achieving higher capacity and robustness.

Authors in [27] proposed method for Embedding and Extraction Process using Random keys. In this paper, they have presented an audio steganography technique based on LWT(Lifting Wavelet Transformation) and modified LSB technique by using three random keys. They used three random keys to increase the robustness of the LSB. The first key is used for embedding the type of the secret message "text or audio or image", the second key is used for embedding the length of the secret message and the third is used for skip some of bits randomly to increase the robustness of the LSB. Authors used CD coefficient because of high frequencies. Also, the SNR values of proposed method are better than other known methods. Where x is the original signal, y is the stego signal, M and N are the numbers of rows and columns of the input signal and R is maximum value of the signal [27]. This method also provides the comparison for signal to noise ratio.

Authors in [28] purposed method information hiding using encryption in audio Steganography. They firstly encrypt the message using cipher techniques in this method; the original plain text is subjected to classical Vigenere cipher followed by double columnar transposition and then also encrypts the audio the audio file is subjected to encryption. Encryption is carried out by transposition in which the orders of the audio frames are changed generating a scrambled audio file. This scrambling is carried out by the random numbers generated by Blum Blum Shub pseudo random number generation algorithm. The random numbers are generated dynamically using BBS algorithm. The first step of encryption is to restrict the magnitude of each random number to the number of audio frames present in the audio by making use of modulo operation. The audio frames are then traversed starting from the very 1st audio frame. Each audio frame is

swapped with another; the latter's frame number being picked by the random number generated at that instant. The procedure is repeated till all the audio frames are exhausted. Subsequently, the encrypted audio file is obtained.

III. PROPOSED METHOD

A. Phase 1

The first phase is related to encrypting the secret data by using modified Vigenere cipher algorithm that is called The Vigenere Square Encryption Algorithm. The primary weakness of classical Vigenere cipher is the repeating nature of its key. Firstly Vigenere cipher encrypts its inputs by using the key and the plaintext as indices into a fixed lookup table called as the Vigenere square. For easy computation, the algorithm first maps letters to numbers: A=1, B=2, ... SPACE=27. As shown in the matrix below, each row in the square is derived from the row above by circularly shifting it one place to the left:

```

1 2 3 4 5 ... 26 27
2 3 4 5 6 ... 27 1
3 4 5 6 7 ... 1 2
...
27 1 2 3 4 ... 25 26

```

To encrypt, replicate the letters in the key so the key and plaintext are the same length. Then, derive each cipher text letter by lookup in the Vigenere square: use the key letter as the row index and the plaintext letter as the column index. If the key K and the plaintext P are n letters long, form the cipher text result C by indexing into the Vigenere square V , as follows:

$$C(n) = V(K(n), P(n))$$

Decryption simply reverses the process, using the key letter to determine the row index and the cipher text letter to determine the column index, which is the plaintext letter. For example:

$$P(n) = \text{FIND}(V(K(n,:),)) = C(n)).$$

B. Phase 2:

In this phase, each character obtained by encrypted message (C) is extracted and the ASCII value of the character is used to generate bit pattern. Each bit of the pattern replaces the last bits of an audio frame by using modified LSB. Each character is then represented by an 8 bit binary number. Thereby, for each character, here we will have 8 consecutive audio frames.

ASCII conversion is as follow:

Character to be embedded – B

ASCII value of B - 66

8 bit binary representation of the ASCII value:
01000010

8 consecutive audio frames in binary format
(consider the 8 bits)

10010010
01010101
10010101
11110011
10100000
11010101

In this phase we have modified Least Significant Bit (LSB) encoding technique in which the encrypted message (C) is embedded into the cover audio making use of deeper layers to embed message by the modified LSB technique. As shown in table:

Table 1: Modified LSB method

1 st MSB	2 nd MSB	3 rd MSB	Secrete
0	0	0	i+1
0	0	1	i+2
0	1	0	i+3
0	1	1	i+4
1	0	0	i+5
1	0	1	i+6
1	1	0	i+7
1	1	1	i+8

In this way algorithm works and embedding is to be done. Some bits from immediate layers also modified so that PSNR values not affected too much.

C. Phase 3:

Last phase is to encrypt the audio file further for more security. This is done by using transposition method. Here Matrix order is provided by the user at run time according to that encryption of secret message inside audio is to be done. In this test value of original and encrypted file are compared. The encryption process will begin with preprocessing segmentation of audio data. Each audio chunk is separated by intervals of bits in which the form of chunks of audio data array will be used as an input in the transposition. Then transposition process will swap the index array for audio encrypt of chunks. Matrix order is to given to cipher audio secret data. The key is going to affect the outcome of exchange index. After index interchangeable, the audio chunks of data will be redeveloped into new audio file as a result of encryption. Then we will decrypt the audio file at another end by use of key.

IV. RESULTS

As per proposed technique we have taken the message to hide, input audio and then efficiency of this method is analyzed. Result portion contains the about original message, key value, cipher data, audio embedding and its results, PSNR, MSE values and computational time. This part highlights on the waveforms obtained as per message and audio file specifications.

```

Command Window
Please enter the Original_text to be encrypted: Hello
Original_text =
Hello
Enter the Key 33
key =
33
ciphertext =
ZGDKKNZ
read a cover audio file
convert cover audio into binary

```

Fig.1. Results of message by using The Vigenere Square Encryption Algorithm.

Type	Wave Sound (.wav)
Size	80KB
Length	3 seconds
Bit Rate	352 kbps

Fig .2. Audio file specifications

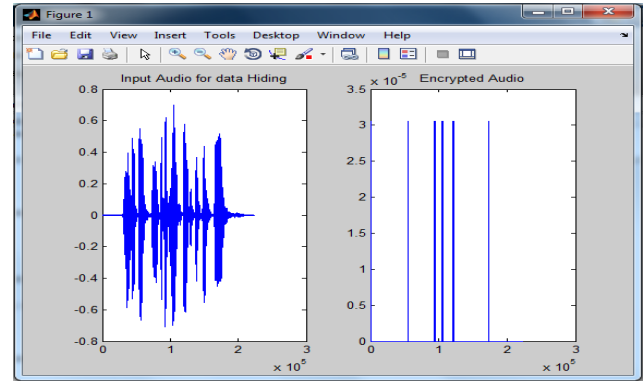


Fig. 3. input audio and encrypted audio using modified LSB method.

```

Command Window
cipher_data =
5 05 05 1 5 5 7 1 1 5 7 7 8 5 5 e 8 8 3- e e .03- 3- 05.0 .0
psnr =
68.6368
mse =
0.0089

```

Fig. 4. results of cipher data using transpositional audio encryption , MSE , PSNR values , extract text and computation time.

```

Please enter the Original_text to be encrypted: nishu

Original_text =
nishu

Enter the Key 33

key =
33

ciphertext =
MHRGT

read a cover audio file
convert cover audio into binary
Press Enter to continue
convert message into binary
Enter the order of Matrix for Transposition Encryption 22

matrix_order =
22

```

Fig.5. Results of another message by using The Vigenere Square Encryption Algorithm

Type	Wave Sound (.wav)
Size	1.20MB
Length	57seconds
Bit Rate	176 kbps

Fig.6. Second Audio file specifications

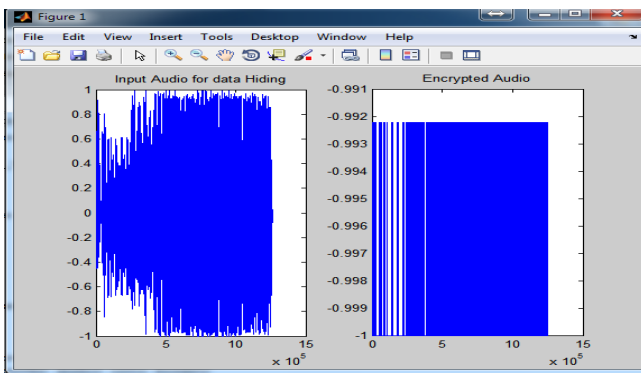


Fig. 7. input audio and encrypted audio using modified LSB method.

```

cipher_data =
-e01+0.009000-e01+0.001+0.000002-e01-0.00000-0.000000-e11+0.000000-e0000-e01+8.000100-e01+
Encrypted audio using Transposition method
PSNR and MSE between Input Audio and Audio with Embedding Data
PSNR and MSE between Input Audio and Encrypted Audio

psnr =
13.5810

mse =
2.8509e+03

Extract_Text =
NISHU

Total_computation_time =
380.9325

```

Fig. 8.results of cipher data using transpositional audio encryption , MSE , PSNR values , extract text and computation time.

Type	Wave Sound (.wav)
Size	1.20MB
Length	57seconds
Bit Rate	176 kbps

Fig.9. Third Audio file specifications

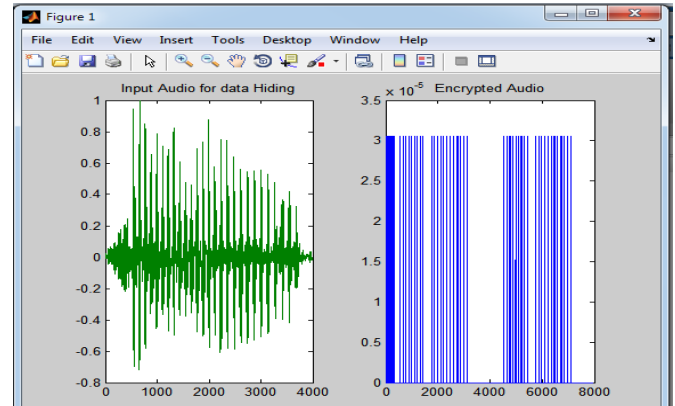


Fig. 10. input audio and encrypted audio using modified LSB method.

AUDIO	CAPACITY(BYTES)	BIT RATE	SNR	MSE(DECRYPTED AUDIO)	COMPUTATIONAL TIME
Gtr-nylon22.wav	1.00 MB	352kbps	79.94	1.0034e-10	36.6482 sec
Hello.wav	350KB	354kbps	91.15	0.0054	56.5055 sec
Input.wav	438KB	706kbps	90.89	0.0089	68.780 sec
Position.wav	750KB	188kbps	87.76	0.0090	68.787 sec
Sheep.wav	980KB	178kbps	85.31	1.0045e-10	97.654 sec
Fonky.wav	1.20MB	176kbps	79.73	2.8509e+03	124.705 sec
Guitar.wav	890KB	352kbps	88.67	0.0092	70.567 sec

Fig. 11 .results after embedding and encryption process

V.CONCLUSION

As discussed above, security of information and data transmitting over the internet is becoming a major concern. In this paper, security for information from intruders using a secure approach of cryptography as well as steganography is there. The secret data is first encrypted which is embedded into an audio file and then this audio file is encrypted before being transmitted over the network. This combination of cryptography and steganography ensures that even if the audio file is intercepted by an unauthorized person, the person doesn't discover the secret information due to steganography and encryption techniques.

As a part of future work, the authors recommend more secure encryption algorithms to be utilized for text encryption. Further, different steganographic techniques can also be used to embed the secret data into stego cover for more security.

ACKNOWLEDGMENT

I would like to express my gratitude to all those who have given me an opportunity to undertake research work in the "AUDIO STEGANOGRAPHY FOR SECURE DATA TRANSMISSION". First of all I am very grateful to my advisor Dr. Amandeep Kaur, Associate Prof. and CoC Centre for Computer Science and Technology, Central University of Punjab, Bathinda. I am extremely thankful to her for sharing expertise, sincere and valuable guidance and encouragement extended to me. I also express my sincere thank you to **Prof. A.K. Jain**, Dean, School of Engineering and Technology, Central

University of Punjab, Bathinda, for the continuous encouragement.

I take this opportunity to express gratitude to my family members and all faculty members for their help and support. I also thank my parents for the unceasing encouragement, support and attention.

REFERENCES

- [1] Forouzan B., "Cryptography and Network Security" special Indian Edition 2007, pp-240-330 Tata McGraw-Hill Publishing Company Limited, New Delhi.
- [2] Suganya.A, Sharmila.R and Gopinathan.N, "A New Method of Secure Communication with Cryptography", International Journal of Computer Sciences and Engineering, Vol.2(4), pp225-228, Apr -2014.
- [3] Sangwan N., "Text Encryption with Huffman Compression", International Journal of Computer Applications (0975 – 8887) Volume 6,pp.54, September 2012.
- [4] Ayushi, "A Symmetric Key Cryptographic Algorithm" International Journal of Computer Applications, Vol. 1(15), pp.-34-37, 2010.
- [5] Wang H. and Wang S., "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, vol. 47,pp.120-156 no. 10, 2004
- [6] Adhiya K. and Patil S., Hiding Text in Audio Using LSB Based Steganography. Information and Knowledge Management, pp.56-98 2012.
- [7] Gilani J., and Khalid M. Asad, "An enhanced least significant bit modification technique for audio steganography", 2011 International Conference on Computer Networks and Information Technology (ICCNIT), pp.230-233 ,IEEE, 2011.
- [8] Gill M.K. and Randhawa R. K., "Comparative Study of Multibit LSB Steganography with Cryptography", International Journal of Computer Sciences and Engineering, Vol.3(7), pp.120-123, Jul -2015.
- [9] Suri S, Joshi H, Mincoha V. and Tyagi A., "Comparative Analysis of Steganography for Coloured Images", International Journal of Computer Sciences and Engineering, Vol.2(4), pp.180-184, Apr -2014
- [10] Bender W. , Gruhl D., "Echo hiding," in proceeding of the 1st Information Hiding Workshop, England, pp. 295-315, 1996.
- [11] Shirali-Shahreza S., "Steganography in Silence Intervals of Speech," in , proceedings of the Fourth IEEE International Conference on Intelligent Information Hiding and Multimedia Signal (IIH-MSP 2008), Harbin , china,pp.78-80, 2008.
- [12] Gopalan S., "Audio Steganography for Covert Data Transmission by Imperceptible Tone Insertion," in WOC, Banff , Canada, pp. 8-10,2004.
- [13] Tapio S. , Cvejic N., "Increasing The Capacity of LSB-Based Audio Steganography," IEEE, 2002.
- [14] Kriti, and Saroha P. , "A variant of LSB steganography for hiding images in audio,," International Journal of Computer Applications, vol.6 , pp. 21-27, 2010.
- [15] Shahadi H. and Jidin R., "High capacity and inaudibility audio steganography scheme," in 7th International Conference n Information Assurance and Security (IAS), IEEE, pp-890-899,2011.
- [16] Bhasker V., Shiva V. Khan S., "An Optimized Method for Concealing Data using Audio Steganography," International Journal of Computer Applications, pp. 0975-8887, 2011.
- [17] Gilani J., Asad A., "Three Layered Model," in International Conference on Emerging, US , pp. 56-78 , 2012.
- [18] Ballesterio D. and Moreno J., "Highly transparent steganography model of speech signals using Efficient Wavelet Masking," vol. 6 ,pp. 48-56 , 2012.
- [19] Katariya V., Patil K., Bankar P., "Audio Steganography using LSB," international Journal of Electronics, vol. 5, pp. 90-92, 2012.
- [20] R A.,Al-Anani M., Al-Khalid R. , & Al-Dallah M., "An Efficient technique for data hiding in audio signals,," American Academic & Scholarly Research Journal, vol. 56 , pp. 10-16, 2012.
- [21] Galshetwar G.,Jeyakumar A., Mane A., "Data Hiding Technique: Audio Steganography using LSB Technique," International Journal of Engineering Research and Applications, vol. 5, pp. 1123-1125, 2012.
- [22] Reddy M. , S.S. Divya, "Hiding Text In Audio Using Multiple LSB Steganography And Provide Security Using Cryptography," International Journal of Scientific & Technology, vol. 4 pp. 68-70, 2012.
- [23] Gaidhani C.R., Deshpande V.M. and Bora V.N., "Image Steganography for Message Hiding Using Genetic Algorithm", International Journal of Computer Sciences and Engineering, Vol.2(3), pp.67-70, Mar -2014.
- [24] Banerjee S., Rana L., "Dual Layer Randomization in Audio Steganography Using Random Byte Position Encoding," International Journal of Engineering and Innovative Technology, vol. 3,pp. 8, 2013.
- [25] John S., B.D, Muruganantham C. and Murthy D., Babu L., "Steganographic Method for Data Hiding in Audio Signals with LSB & DCT," International Journal of Computer Science and Mobile Computing, vol.2, pp. 89-93, August 2013.
- [26] Prof. Trivedi.V., Jain M., "Effective Audio Steganography by using Coefficient Comparison in DCT Domain," International Journal of Engineering Research & Technology (IJERT), vol 2 pp. 45-51, 2013.
- [27] Nasef M. and Fatma T. , Eid Meligy A., "An Efficient Method to Audio Steganography based on Modification of Least Significant Bit Technique using Random Keys," I. J. Computer Network and Information Security, vol .4, pp. 24-29, 2015.
- [28] Bhowmick A., Kishore B., Sinha N., "Encrypted Information Hiding using Audio Steganography and Audio Cryptography," International Journal of Computer Applications, vol. 2 , pp. 0975-8123, 2015.

Authors Profile

Miss **Nisha Kundu**, received B.Tech degree from MDU Rohtak, India. She is pursuing M.tech (final semester) in Computer Science and Technology(Cyber Security) from Central University of Punjab, Bathinda, India. She has two research publications and one conference paper during M.tech. She has more than one year teaching experience in polytechnical college after graduation. Her main area of interests in research is Steganography , Cryptography, network security , algorithms etc..

Dr. Amandeep Kaur is associate professor at central university of punjab. She has more than 15 year work experience in teaching. She has more than 17 research publications .Her main interest of research is in fuzzy logics, neural networks , steganography , image processing etc.